Physical secure optical communication based on private chaotic spectral phase encryption/decryption

Jiang, Ning; Zhao, Anke; Xue, Chenpeng; Tang, Jianming; Qiu, Kun

Optics Letters

DOI:
10.1364/OL.44.001536

Published: 01/04/2019

Peer reviewed version

Physical secure optical communication based on private chaotic spectral phase encryption/decryption

NING JIANG,[1,2*] ANKE ZHAO,[1] CHENPENG XUE,[1,2] JIANMING TANG,[2] KUN QIU[1]

1School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China
2 School of Electronic Engineering, Bangor University, Dean Street, Bangor LL57 1UT, UK
**Corresponding author: uestc_nj@uestc.edu.cn*

Received XX Month XXXX; revised XX Month, XXXX; accepted XX Month XXXX; posted XX Month XXXX (Doc. ID XXXXX); published XX Month XXXX

We propose and demonstrate a novel physical secure high-speed optical communication scheme based on synchronous chaotic spectral phase encryption (CSPE) and decryption (CSPD). The CSPE is performed by a module composed of two dispersion components and one phase modulator (PM) between them, and the CSPD is carried out by a twin module with reverse dispersions and inverse PM driving signals. The PM driving signals of the CSPE and CSPD modules are privately-synchronized chaotic signals that are independently generated by local external-cavity semiconductor lasers subject to common injection. The numerical results indicate that with the CSPE, the original message can be encrypted as a noise-like signal, and the timing clock of original message is efficiently hidden in the encrypted signal. Based on the private synchronization of the chaotic PM driving signals, only the legal receiver can decrypt the message correctly, while the eavesdropper is not able to intercept useful message. Moreover, the proposed scheme can also support secure symmetric bidirectional high-speed WDM transmissions. This work shows a prospective way to implement high-speed secure optical communications at physical layer. © 2019 Optical Society of America

http://dx.doi.org/10.1364/OL.99.099999

In recent years, along with the unprecedented fast developments in communications and computer technologies, the information security risks grow considerably, which has attracted worldwide extensive attention [1]. While most of the previously published security enhancement strategies are based on algorithm encryption, such as the typical AES. Due to the deterministic characteristic of algorithms, this kind of encryption is facing a significantly serious threat since with sufficiently fast computation ability, such as the emerging quantum computation, the encrypted message may still be intercepted by an exhaustive attack. Therefore, it is greatly important and timely to explore advanced physical encryption with nondeterministic characteristics to further enhance the security of communication systems.

To address the abovementioned challenges in the field of optical communications, several physical security strategies, such as quantum communications [2,3], chaos communications [4-7] and optical code division multiple access (OCDMA) have been reported [8,9]. However, due to the stringent device requirements and the limited rate of quantum key distribution, the quantum encryption is not suitable for the present high-speed optical communications [2]. Regarding the chaos communications that utilizes the intrinsic information hiding characteristic of chaos, due to the limited bandwidth of chaotic carrier, it can only support maximum transmission bit rates up to about 10 Gbit/s [10], and meanwhile, when the message bit rate is low, the encryption efficiency of chaos communications is relatively low, the message may be intercepted by the attack ways of direct detection linear filtering and utilization of synchronization [11,12]. OCDMA is another way of using physical effect for encryption, the security of communication is based on overlapping multiple channels in the same frequency space. Nevertheless, it would induce substantial measurement burden for the specific optical domain encoding and decoding, and its practical security is still an open question [13]. From a different perspective, in this paper we propose a high-speed physical secure optical communication scheme based on chaotic spectral phase encryption (CSPE), in which distributed privately-synchronous chaotic signals are used as the secret key to encrypt (decrypt) the message signal as (from) a noise-like signal. The proposed secure scheme supports secure high-speed bidirectional WDM transmission on the physical layer, and it is inherently transparent to the modulation formats and can be flexibly compatible with the existing optical communication systems.

Figure 1 shows a configuration of the proposed secure optical communication scheme. At the transmitter (Alice) end, the message is firstly modulated into a continuous-wave (CW) optical carrier by a typical intensity modulator (IM). Any modulation formats, such as OOK, QPSK, QAM are applicable. After that, the optical message signal is sent into a CSPE module which is composed of two dispersion components (D1 and D2) and one phase modulator (PM) between them. D1 is used to intensively distort the message signal in the time domain, the PM is adopted to expand the spectrum in the optical domain, and D2 is used to convert the spectrum-expanded phase signal into intensity. D1 and

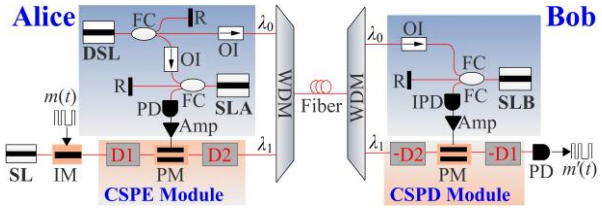

Fig. 1. Schematic of the proposed secure optical communication system based on the private CSPE/D. SL, semiconductor laser; DSL, driving SL; IM, intensity modulator; PM, phase modulator; Amp, RF amplifier; (I)PD: (inverse) photodetector; OI, optical isolator; D, dispersion component; FC, fiber coupler; R, reflector; $m(t)$, original message; $m'(t)$, recovery message.

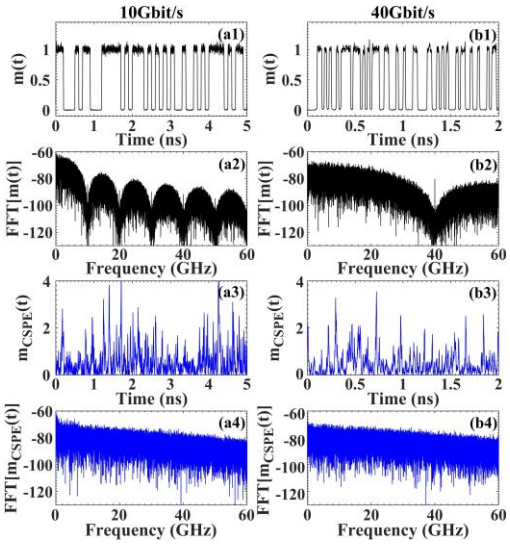

Fig. 2. Temporal waveforms and RF spectra of the OOK message signal before (black) and after (blue) the CSPE for the cases of 10 Gbit/s (first column) and 40Gbit/s (second column) transmissions.

D2 can be constructed with dispersion fiber or fiber grating, and the PM driving signal is a chaotic signal which is photon-detected from the output of a local chaotic external cavity semiconductor laser (ECSL) SLA that is subject to injection from a driving chaotic laser DSL. The configuration of the CSPE is similar to that of the fractional Fourier transformation (FRFT) in [14] and the spectral phase encoding for OCDMA system reported in [15]. However, the FRFT requires identical and negative dispersion coefficients for the dispersion components and positive sinusoidal PM driving signal [14], and the spectral phase encoding is performed with two dispersion components with opposite dispersion coefficients and a PM driven by orthogonal binary optical codes [15]. Nevertheless, in the proposed CSPE, the PM is driven by private chaotic signal, and the dispersions of D1 and D2 can be set independently and arbitrarily. With the joint effects of the dispersion and the chaotic phase modulation, the message signal is encrypted as a totally different signal in both of time domain and frequency domain, thus we refer this encryption as the CSPE. At the receiver (Bob) end, a twin chaotic spectral phase decryption (CSPD) module with two dispersion components having opposite signs (-D2 and -D1) and a PM driven by an inverse chaotic driving signal is adopted to decrypt the message. The PM driving signal for the CSPD is the output of a local ECSL SLB which is identical to SLA and subject to identical chaotic injection from DSL. The chaotic injection signal of SLB is transmitted along with the encrypted signal, in virtue of the WDM technique. Similar to the common-signal-induced chaos synchronization for secure key distribution reported in [16,17], with proper selections of the strength of chaotic injection from DSL and the feedback strengths of SLA and SLB, the chaotic outputs of SLA and SLB can be well synchronized but different from that of DSL, which guarantees the privacy of CSPE and CPSD, and hence provides high-level physical security for the message transmission. It is worth mentioning that the dispersion of transmission link can be regarded as one part of -D2, and thus no extra dispersion compensation for the transmission link is necessary. In addition, since the CPSE and CPSD modules can be plugged-in and pulled-out freely, the proposed physical security technique can be flexibly compatible with existing optical communication systems.

Simulations are jointly performed on the VPIphotonics and the Matlab software. The intrinsic parameters of DSL, SLA and SLB are set as the representative values of typical SLs reported in [5,18], and their operation wavelengths are set as 1553.2 nm. The bias current, feedback strength and feedback delay of DSL are set as 29 mA, 20 ns^{-1} and 3 ns, respectively, while those of SLA and SLB are chosen as 22 mA, 15 ns^{-1}, and 2 ns, respectively. The injection strength from DSL to SLA and SLB are chosen as 50 ns^{-1}. The CW laser is a DFB laser working at 1550 nm with a linewidth of 10 MHz, an output power of 1mW, a side-mode suppression ratio of 30 dB, and a relative intensity noise (RIN) level of -150 dB/Hz. The half-voltage of the PM is 4 V, and the peak amplitude of chaotic PM driving signal is 6 V. The transmission link is a 50 km single mode fiber with a dispersion coefficient of 16 ps/nm/km and a loss coefficient of 0.2 dB/km. A semiconductor optical amplifier with a centralized wavelength of 1550 nm, a 3-dB bandwidth of 30 nm, an optical gain of 10 dB and a noise figure of 7 dB, is adopted to compensate the transmission-induced attenuation at the receiver end. The noise figures of the photodetectors and the electronic amplifiers are set as 10^{-12} $A/Hz^{-1/2}$. The dispersion components for the CSPE and the CSPD are constructed using dispersive fibers. Specifically, D1 is a dispersive fiber with a length of 2 km and a dispersion coefficient of 500 ps/nm/km, and D2 is a similar dispersive fiber with a length of 3 km. The dispersion coefficients of –D1 and –D2 are opposite to those of D1 and D2, and the length of -D1 is 2km, while the length of -D2 is 4.6 km (500 ps/nm/km × 3 km + 16 ps/nm/km × 50 km = 500 ps/nm/km × 4.6 km), which takes the compensation for the transmission link dispersion into consideration. In addition, for the sake of simplicity, the modulation format of message is set as OOK.

Figure 2 illustrates the process of CSPE for the transmission cases with typical bit rates of 10 Gbit/s and 40 Gbit/s. Apparently, in the time domain, the original regular OOK messages shown in Figs. 2 (a1) and (b1) are converted into totally different noise-like signals, which means the original messages are efficiently hidden in the encrypted signal. Simultaneously, in the frequency domain, the RF spectra of encrypted signals are much flatter and wider than those of original signals. Moreover, the intrinsic timing clocks (the peaks at the positions of bit rate and its harmonic frequencies in Figs. 2(a2) and 2(b2)) in the original messages are efficiently hidden in the flat-spectrum encrypted message, which also greatly

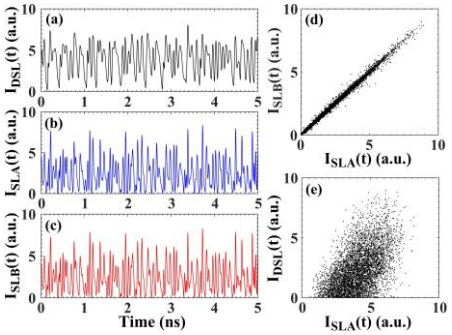

Fig. 3. Temporal waveforms of the chaotic signals generated by (a) DSL, (b) SLA and (c) SLB, as well as the cross-correlations of (d) SLA-SLB and (e) DSL-SLA. Since the cross-correlation of DSL-SLB is similar to that of DSL-SLA, it is not shown here for simplicity.

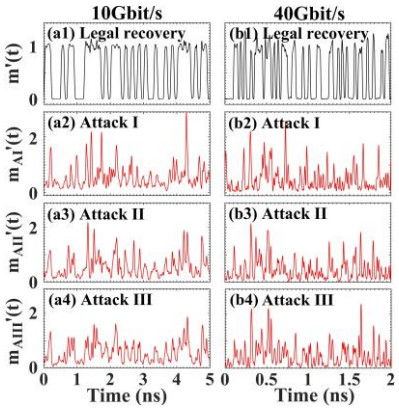

Fig. 4. Illustrations of the message recovery under the scenarios of legal CSPD (first row), direct detection attack (second row), illegal CSPD with injection chaos (third row), and illegal CSPD with chaos generated by solitary laser subject to chaos injection as SLA (SLB), for the 10Gbit/s and 40Gbit/s transmission scenarios.

increases the difficulty of interception, because without the timing clock of original message, the eavesdropper cannot process the intercepted signal with precise sampling, let alone recover correct message. Therefore, with the proposed CSPE, the message can be well hidden in the encrypted signal, it is extremely difficult for the eavesdropper to intercept the message by directly analyzing the noise-like encrypted signal.

The chaos synchronization between SLA and SLB is the key to decrypt the message from the noise-like transmission signal. Figure 3 presents the temporal waveforms of the chaotic signals outputted by DSL, SLA and SLB, as well as the cross-correlation functions between them. It is indicated that the chaotic outputs of SLA and SLB are well synchronized with a correlation coefficient (CC) of 0.99, while the cross-correlation between them and the injection chaos from DSL is relatively low (CC=0.57). The high-quality chaos synchronization between SLA and SLB guarantees the successful decryption of message, and simultaneously the low cross-correlation between DSL and SLA (SLB) guarantees the privacy of the chaotic PM driving signals. Since the chaotic PM driving signals are independently generated by the local lasers SLA and SLB, and only the chaos injection from DSL is transmitted over the public link, the eavesdropper cannot obtain precise chaotic PM driving signals from the injection, as such he cannot intercept the message, which will be confirmed in the following discussions.

Next, we turn to investigate the message transmission between Alice and Bob, on the basis of the private CSPE and CSPD. Figures 4(a1) and 4(b1) show the decrypted messages with synchronous CSPD, for the 10Gbit/s and 40Gbit/s transmission cases. Obviously, with the synchronous CSPD, the original messages shown in Figs. 2(a1) and 2(b1) are correctly recovered. Moreover, to visually demonstrate the system security against illegal interceptions, here we consider three indicative attack scenarios, which are described as follows. Attack I: the eavesdropper intercepts the message by directly detecting the public link signal (encrypted signal). Attack II: the eavesdropper uses the chaos injection from DSL as the PM driving signal of CSPD, to intercept the message. Attack III: the eavesdropper injects the chaotic signal from DSL into a solitary laser (no feedback) with intrinsic parameters that are identical to those of SLA and SLB, to generate a local chaotic PM driving signal for the CSPD to intercept the message. Here it is assumed that the eavesdropper knows the message bit rate, although it has been confirmed that the timing clock can be totally hidden by the CSPE [Figs. 2(a4) and 2(b4)]. Apparently, with respect to the original and legally-decrypted messages, the intercepted messages under these attack scenarios are chaotic, no useful message is recovered. That is, the proposed physical secure optical communication system can defend these attacks.

To systematically study the communication performance and security of the proposed scheme, we present the Q-factor of the messages recovered by the legal CSPD and the abovementioned attacks, versus the bit rate of message in Fig. 5. The definition of Q-factor is identical to those in [5,17]. Under the legal CSPD scenario, although the Q-factor of the recovery message gradually decreases with increasing bit rate of message, an acceptable communication performance with a Q-factor around 6 can be maintained for the high-speed transmissions with a bit rate as high as 100Gbit/s. However, for the illegal attacks, the Q-factors of the recovery messages always keep at a very low level, even when the bit rate of message is low. The significant difference between the legal decryption and the illegal attacks can be more directly observed by comparing the eye diagrams of the messages recovered by the legal decryption and the illegal attacks shown in Figs. 5(b1)-5(c4). Therefore, it can be concluded that the proposed scheme supports high-speed secure optical communications.

In the proposed scheme, due to the symmetric configurations, the CSPE (CSPD) module can work as the CSPD (CSPE) module for the opposite direction communication. Simultaneously, since the dispersive components and PMs in the CSPE and CSPD modules can work in a wide range of wavelength, the proposed scheme can also support WDM transmissions. Based on these properties, high-speed secure bidirectional WDM communications is achievable. Here we take one bidirectional WDM transmission case with 7 wavelengths centralized at 1550 nm and a typical channel spacing of 0.8 nm for instance. Figure 6 shows the Q-factors of decrypted messages versus the bit rate of message, under the bidirectional WDM communication scenario. It is shown that in both directions the communication performances show similar developing trends. For the central wavelength channel (Ch.0) and its two nearby channels (Ch.+1 and Ch.-1), when the bit rate of message is lower than 70 Gbit/s, satisfactory communication performance with Q-

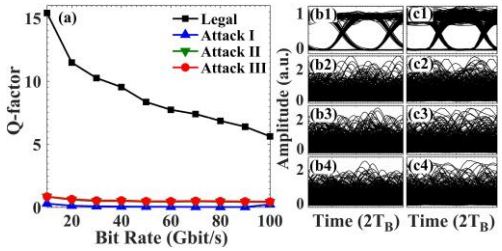

Fig. 5. (a) Q-factor of the messages recovered by legal decryption and illegal attacks, versus the bit rate of message. The second column (b1)-(b4) and the third column (c1)-(c4) show the eye diagrams of the legal and illegal recovery messages, for the 10 Gbit/s and 40 Gbit/s transmission cases, respectively. T_B is the bit period of message, which is the reciprocal of bit rate.

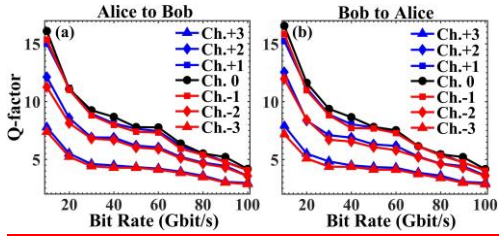

Fig. 6. Performance (Q-factor of recovery message) of bidirectional WDM communication in (a) the direction from Alice to Bob and (b) the opposite direction, versus the bit rate of message. Ch.0 stands for the central wavelength channel at 1550 nm, Ch.±*i* denotes the side channels with wavelengths of 1550±0.8*i* nm (*i*=1, 2 and 3).

factors greater than 6 can be maintained. With respect to the single channel transmission scenario shown in Fig. 5, the communication performances on these three channels is slightly degraded when the message bit rate is relatively high (higher than about 60 Gbit/s), for the channel interferences. While for the far-from-central-wavelength channels, namely the Ch.+2, Ch.-2, Ch.+3 and Ch.-3, the Q-factor performances are degraded, comparing with that of Ch.0. The transmission capacities (bit rate range in which the Q-factor is greater than 6) of these channels are also degraded to 60 Gbit/s, 60 Gbit/s, 10Gbit/s and 10 Gbit/s, respectively. The performance degradation on the far-from-central-wavelength channels is attributed to that the dispersion considered into -D2 is evaluated by the transmission dispersion on central wavelength channel. For the channels nearby central wavelength channel, the transmission dispersions on these channels are similar to that of the central wavelength channel, thus the performances on these channels are similar to that of central wavelength channel. While for the far-from-central-wavelength channels, the dispersion considered into -D2 is not so accurate as the transmission dispersions, as such the transmission dispersions on these channels cannot be totally compensated. Consequently, the decryption performances on these channels are degraded by the residual transmission dispersion-induced distortions. Although the CPSD cannot support a large number of WDM channels, secure bidirectional WDM transmission with a capacity of hundreds of Gbit/s in each direction is achievable, by utilizing the nearby-central-wavelength channels. In fact, when the number of WDM channels is large, the proposed technique can also be feasible, by dividing the WDM channels into different groups and in each group a pair of CSPE and CSPD working at the central wavelength of the corresponding group is used to achieve high-speed secure optical communication.

In conclusion, we proposed a secure optical communication scheme that supports high-speed bidirectional WDM transmission, by introducing a pair of CSPE and CSPD modules that use privately synchronized chaotic signals as the secret key for encryption and decryption into conventional optical communication system. It is numerically demonstrated that with the CSPE, the original message can be encrypted as a noise-like signal, and the intrinsic timing clock of message can be efficiently hidden. In virtue of the private synchronous CSPE and CSPD, only the legal receiver can efficiently decrypt the message, while the eavesdroppers cannot. Moreover, the proposed scheme not only supports secure high-speed transmission up to 100 Gbit/s on single channel, but also allows for simultaneous bidirectional secure WDM transmissions with capacity as large as hundreds of Gbit/s. The proposed physical secure communication scheme shows several salient features including inherent transparency to modulation formats, bidirectional WDM transmission suitability, plug-and-play in conventional optical communication systems and use of existing dispersion compensation modules.

Funding. National Natural Science Foundation of China (NSFC) (61671119, 61471087)

References

1. S. Aftergood, Nature **547**, 30 (2017).
2. E. Diamanti, H. W. Lo, B. Qi, and Z. L. Yuan, Quantum Information. **2,** 16025 (2016).
3. F. Xu, M. Curty, B. Qi, and H. K. Lo, IEEE J. Sel. Topics in Quantum Electron. **21**, 6601111 (2017).
4. N. Q. Li, H. Susanto, B. Cemlyn, I. D. Henning, and M. J. Adams, Opt. Lett. **42**, 3494 2017).
5. N. Jiang, A. K. Zhao, S. Q. Liu, C. P. Xue, and K. Qiu, Opt. Express **26**, 32404 (2018).
6. T. T. Hou, L. L. Yi, X. L. Yang, J. X. Ke, Y. Hu, Q. Yang, P. Zhou, and W. S. Hu, Opt. Express **24**, 23439 (2016).
7. A. Argyris, E. Grivas, A. Bogris, and D. Syvridis, J. Lightw. Technol. **28**, 3107 (2010).
8. G. Di Crescenzo, R. Menendez, and S. Etemad, *in Optical Fiber Communication Conference/National Fiber Optic Engineers Conference, OSA Technical Digest 2008* (Optical Society of America, 2008), p. OTuP3.
9. X. Wang, Z. S. Gao, N. Kataoka, and N. Wada, Opt. Express **18**, 9879 (2010).
10. R. Lavrov, M. Jacquot, and L. Larger, IEEE J. Quantum Electron. **46**, 1430 (2010).
11. A. Bogris, A. Argyris, and D. Syvridis, IEEE J. Quantum Electron. **46**, 1421 (2010).
12. C. Xue, N. Jiang, Y. Lv, C. Wang, G. Li, S. Lin, and K. Qiu, Opt. Lett. **41**, 3690 (2016).
13. G. S Kanter, *in Conference on Lasers and Electro-Optics, OSA Technical Digest 2010* (Optical Society of America, 2010), p. CFC3.
14. M. F. Chen, L. Deng, H. Li, and D. M. Liu, Opt. Express **22**, 5241 (2014).
15. X. Wang, and N. Wada, Opt. Express, **15**(12), 7319-7326 (2007).
16. N. Jiang, C. Xue, D. Liu, Y. Lv, and K. Qiu, Opt. Lett. **42**, 1055 (2017).
17. T. Sasaki, I. Kakesu, Y. Mitsui, D. Rontani, A. Uchida, S. Sunada, K. Yoshimura, and M. Inubushi, Opt. Express **25**, 26029 (2017).
18. D. Kanakidis, A. Argyris, A. Bogris, and D. Syvridis, J. Lightw. Technol. **24**, 335 (2006).

1. S. Aftergood, "Cybersecurity: The cold war online," Nature **547**(7661): 30-31(2017).
2. E. Diamanti, H. W. Lo, B. Qi, and Z. L. Yuan, "Practical challenges in quantum key distribution," Quantum Information. **2,** 16025 (2016).
3. F. Xu, M. Curty, B. Qi, and H. K. Lo, "Measurement-device-independent quantum cryptography," IEEE J. Sel. Topics in Quantum Electron. **21**(3), 6601111 (2017).
4. N. Q. Li, H. Susanto, B. Cemlyn, I. D. Henning, and M. J. Adams, "Secure communication systems based on chaos in optically pumped spin-VCSELs," Opt. Lett. **42**(17), 3494-3497 (2017).
5. N. Jiang, A. K. Zhao, S. Q. Liu, C. P. Xue, and K. Qiu, "Chaos synchronization and communication in closed-loop semiconductor lasers subject to common chaotic phase-modulated feedback," Opt. Express **26**(25), 32404-32416 (2018).
6. T. T. Hou, L. L. Yi, X. L. Yang, J. X. Ke, Y. Hu, Q. Yang, P. Zhou, and W. S. Hu, "Maximizing the security of chaotic optical communications," Opt. Express **24**(20), 23439-23449 (2016).
7. A. Argyris, E. Grivas, A. Bogris, and D. Syvridis, "Transmission effects in wavelength division multiplexed chaotic optical communication," J. Lightw. Technol. **28**(21), 3107-3114 (2010).
8. G. Di Crescenzo, R. Menendez, and S. Etemad, "OCDM-based photonic encryption with provable security," in Optical Fiber Communication Conference/National Fiber Optic Engineers Conference, OSA Technical Digest 2008 (Optical Society of America, 2008), p. OTuP3.
9. X. Wang, Z. S. Gao, N. Kataoka, and N. Wada, "Time domain spectral phase encoding/DPSK data modulation using single phase modulator for OCDMA application," Opt. Express **18**(10), 9879-9890 (2010).
10. R. Lavrov, M. Jacquot, and L. Larger, "Nonlocal nonlinear electro-optic phase dynamics demonstrating 10Gb/s chaos communications," IEEE J. Quantum Electron. **46**(10), 1430-1435 (2010).
11. A. Bogris, A. Argyris, and D. Syvridis, "Encryption efficiency analysis of chaotic communication systems based on photonic integrated chaotic circuits," IEEE J. Quantum Electron. **46**(10), 1421-1429 (2010).
12. C. Xue, N. Jiang, Y. Lv, C. Wang, G. Li, S. Lin, and K. Qiu, "Security-enhanced chaos communication with time-delay signature suppression and phase encryption," Opt. Lett. **41**(16), 3690-3693 (2016).
13. G. S Kanter, "Secure optical communication," in Conference on Lasers and Electro-Optics, OSA Technical Digest 2010 (Optical Society of America, 2010), p. CFC3.
14. M. F. Chen, L. Deng, H. Li, and D. M. Liu, "Enhanced secure strategy for electro-optic chaotic systems with delayed dynamics by using fractional Fourier transformation," Opt. Express **22**(5), 5241-5251 (2014).
15. X. Wang, and N. Wada, "Spectral phase coding of ultra-short optical pules in time domain for OCDMA application," Opt. Express, **15**(12), 7319-7326 (2007).
16. N. Jiang, C. Xue, D. Liu, Y. Lv, and K. Qiu, "Secure key distribution based on chaos synchronization of VCSELs subject to symmetric random-polarization optical injection," Opt. Lett. **42**(6), 1055-1058 (2017).
17. T. Sasaki, I. Kakesu, Y. Mitsui, D. Rontani, A. Uchida, S. Sunada, K. Yoshimura, and M. Inubushi, "Common-signal-induced synchronization in photonic integrated circuits and its application to secure key distribution," Opt. Express **25**(21), 26029-26044 (2017).
18. D. Kanakidis, A. Argyris, A. Bogris, and D. Syvridis, "Influence of the decoding process on the performance of chaos encrypted optical communication systems," J. Lightw.Technol. **24**(1), 335–341 (2006).